Teaching Aggressive Information Security Labs

Presented by Scott Cote'
On Behalf of Scott Roberts
WECS 7, Naval Postgraduate School, January 2006

CiSR

The Center for Information Systems Security Studies and Research

WECS 7 Seventh Workshop on Education in Computer Security

Presenting for Scott Roberts

- Scott Roberts regrets he will be unable to present today at the WECS7 conference.
- Please be sure to read his paper in the proceedings on *"Adding When, Where, and Why to How: Providing Ethical Context in Aggressive Information Security Labs."*

Quick Background on Scott Cote'

- Been lecturing on vulnerability assessment techniques since the Summer of 2003.

CND CNA HACKERS NMAP ROOT SCANNING ENUMERATION
VULNERABILITY ASSESSMENT
GSOIS AT THE NAVAL POSTGRADUATE SCHOOL
CS3675

- Attended Blackhat and DEFCON on multiple occasions, and has participated on the CTF (Capture the Flag) competition there twice.

Teaching Aggressive Labs?

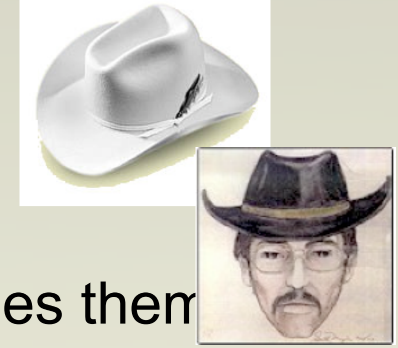
Tools such as: NMAP, L0pht Crack, Nessus...

How many teach them now: (#/#)

How many are planning on teaching
them in the future, or would like to: (#/#)

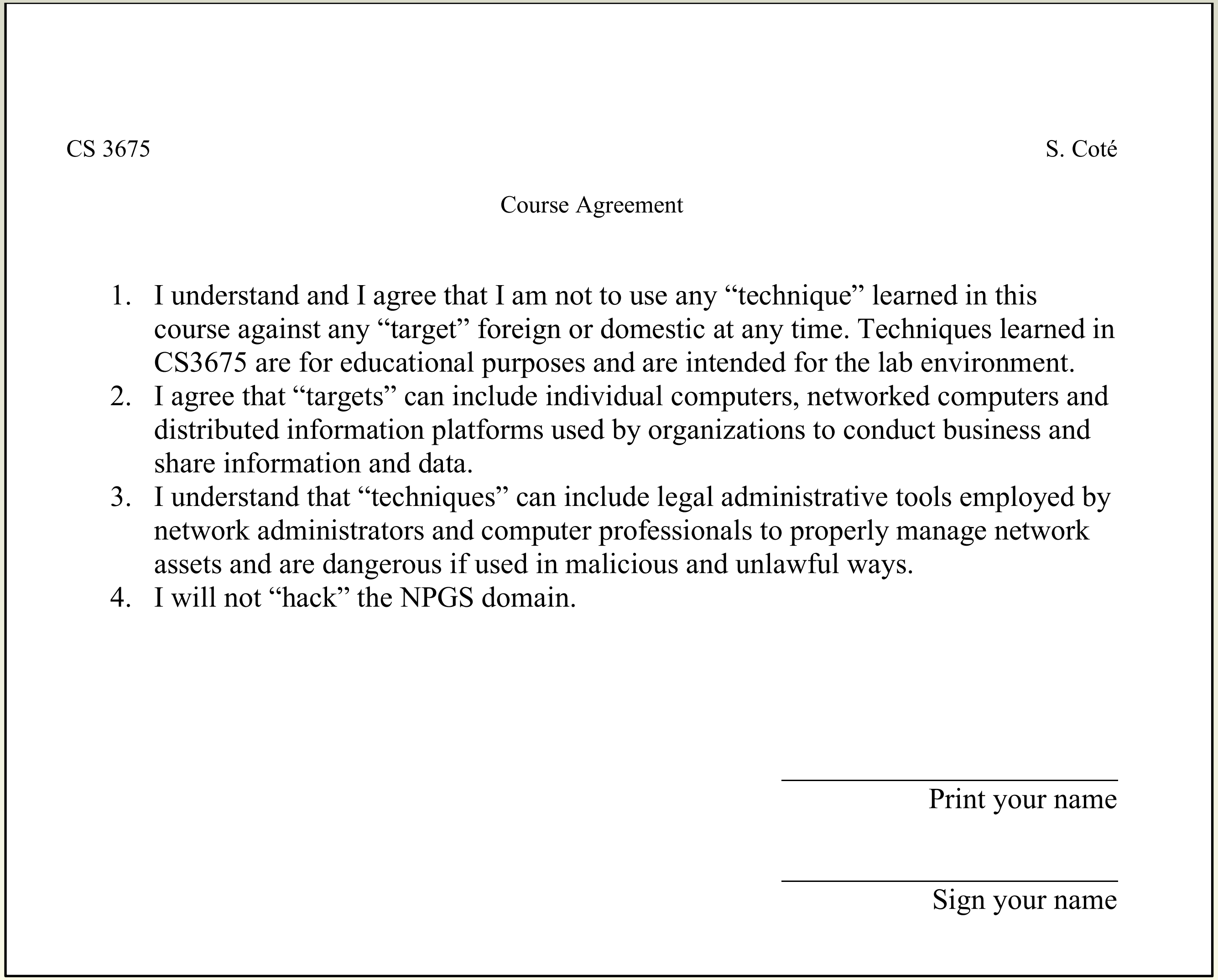
Reasons To Teach Them:	Reasons NOT To Teach Them:

When You Do Teach Them...



- **MUST reinforce the concepts of ethical use!**
  - Tools themselves are _*not*_ inherently evil
    - Its how they are used! The motivation!
  - Like cops and bad guys, both carry guns, but one uses them only in support of the safety of others, not for selfish reasons.
- **Place them in the context of how real-world security professionals use them.**
  - Self-assessing ones own vulnerabilities
    - Crack ones own organization’s passwords for weak ones
    - Scanning ones own network for vulnerabilities
    - Understanding how new methods and tools can be used against your organization!
  - _*Have lab write-ups reflect the format of an audit report you would submit to superiors in an organization!*_
- _***Have them sign a course agreement!***_

Sample Course Agreement



CS 3675 S. Coté

Course Agreement

1. I understand and I agree that I am not to use any “technique” learned in this course against any “target” foreign or domestic at any time. Techniques learned in CS3675 are for educational purposes and are intended for the lab environment.
2. I agree that “targets” can include individual computers, networked computers and distributed information platforms used by organizations to conduct business and share information and data.
3. I understand that “techniques” can include legal administrative tools employed by network administrators and computer professionals to properly manage network assets and are dangerous if used in malicious and unlawful ways.
4. I will not “hack” the NPGS domain.

____
Print your name

____
Sign your name

Open Discussion

Some Other Tid-bits to Know

- The next few slides may not be covered during the session, time permitting, but I include them as I find them interesting and are relevant to the discussion...

So Why Do They Hack?

- Script Kiddies:
  - According to Sarah Gordon, antivirus expert and hacker profiler:
    - Kids socialize via the Internet, communicating without having to really connect as you do in person. This creates a type of "cover" removing them from the real world.
    - Kids are curious… computers are a great place to exercise that curiosity.
      - *My personal experience: Letting the genie out of the bottle tends to take the mystery out, and they loose interest.*
    - This type of virtual world removes one from the consequences of our actions (such as the damage caused by releasing a virus).
    - Most come to realize the damage, and tend to age out of it.

So Why Do They Hack?

- Sarah continues:
- Hackers get away from scripts and into actually understanding the computer…
  - Hackers don’t generally age out of it, but find legitimate ways to use their talents.
  - Curiosity again is the motivation of a good hacker…

So Why Do They Hack?

- Author Donn Parker "*Fighting Computer Crime*"
- Cyber-criminals have *intense* personal problems…
  - Need to rationalize their crimes
    - *"The bank desperately needed my consulting services but did not realize it"*
    - *"Its okay to break the laws of foreign countries, as long as its not your own, especially of they are richer then your country"*

So Why Do They Hack?

- Author Donn Parker "*Fighting Computer Crime*"
- They exhibit *differential association syndrome* … "everyone does it"
- Many anthropomorphize the computers they attack… viewing the computers as adversaries and deriving some enjoyment from ripping them off
- Robin Hood syndrome

So Why Do They Hack?

- Parker’s common traits of youthful hackers
  - Precociousness, curiosity, persistent
  - Habitual lying, cheating, exaggerating
  - Juvenile idealism, e.g. “power to the people”
  - Hyperactivity
  - Drug and alcohol abuse

So Why Do They Hack?

- Parker's states:
- *"In today's hacker culture, malicious hackers regularly engage in fabrications, exaggerations, thievery and fantasy… presenting themselves to the media and general public as idealistic do-gooders…their role as Clark Kent who become Supermen of cyberspace…Although malicious hackers range in age from preteens to senior citizens, they are characterized by an immature excessively idealistic attitude… they act like irresponsible kids playing cops and robbers in a fantasy world that can suddenly turn real when they are caught"*

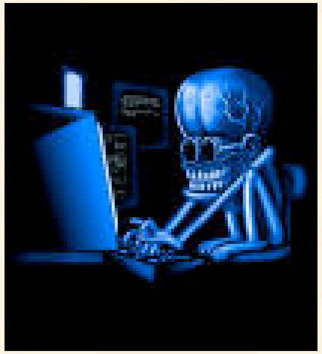
Hackers vs Crackers

- There is a difference!!
- Hackers:
  - Gifted person who extends the function of a computer beyond its original design
  - Hackers are basically GOOD…
- Crackers:
  - Maliciously attack computer systems!
  - Crackers are basically BAD…

http://pls.mrnet.pt/headline4visual1.html

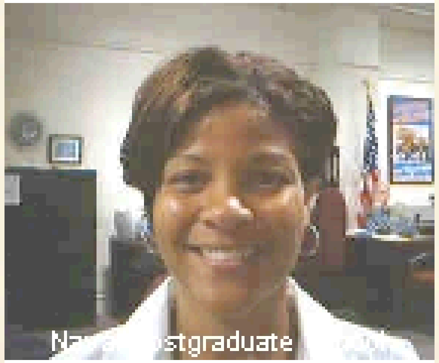
Hacker Stratification

As seen by Stuart McClure

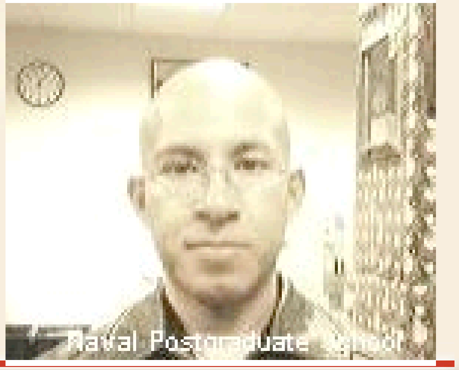


- Tier I
  - Best of the best
  - Find new vulnerabilities
  - Write their own exploit code and tools

Hacker Stratification

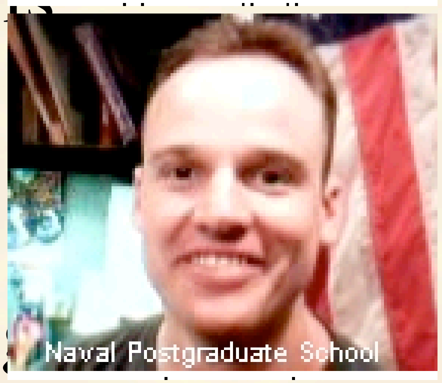


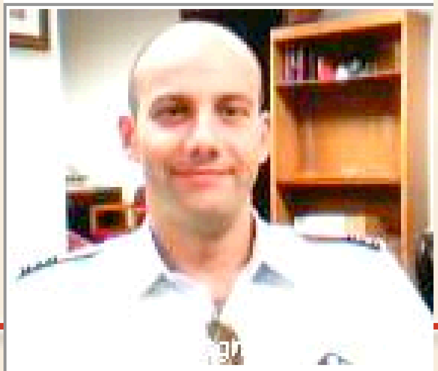
- Tier II
  - IT Savvy
  - Ability to program or script
  - Understand what the vulnerability is and how is works...
  - Intelligent enough to use the exploit code and tools with precision



Hacker Stratification

- Tier III
  - “Script Kiddies” (Inexpert)
  - ability to down load exploit code and too
  - Very little understanding of the actual vulnerability
  - Randomly fires off scripts until somethin works...





So What Color Hat Do You Wear?

- White Hats:
  - Computer Security Experts
  - Find and Fix Vulnerabilities
- Black Hats:
  - Malicious Attackers
  - Break into Systems